IN THE CLAIMS:

Please cancel claims 1 - 6 in their entirety and without prejudice and substitute the following new claims:

A4

--7. A method for verifying the usage of public keys derived from a set of asymmetric keys, a public key (Kp) and private key (Ks) generated for a given use, such as encryption/decryption or digital signature verification/generation, by an on-board system and stored in the storage area of an on-board system (S_i) equipped with cryptographic calculation means and externally accessible read/write-protected means for storing digital data, said digital data (IDd_i) comprising at least a serial number (SN_i) for identifying the on-board system and an identification code (Op_j) of an operator authorized to configure said on-board system, the request being formulated by said on-board system by transmitting a request message (MRCA) containing said public key (Kp) to a certification authority (CA), comprising:

PRIOR TO ANY TRANSMISSION OF A CERTIFICATION REQUEST, DURING THE CONFIGURATION OF A SET (Lk) OF ON-BOARD SYSTEMS (S_i) BY THE AUTHORIZED OPERATOR:

- generating by the authorized operator, for said set of on-board systems, a mother public key (KpM) and a mother private key (KsM) used in connection with a process supported by an algorithm (CA1M);
- publishing said mother private key (KpM) associated with the algorithm (CA1M), the identification code of said authorized operator (OP_j), and defining a range of on-board system identifiers for the set (Lk) of on-board systems;
- calculating, for each on-board system of said set (Lk) of on-board systems,

from said mother private key (KsM) and from the serial number (SN_i) of the on-board system, a diversified private key (KsM_i), and storing said diversified private key (KsMi) in said externally accessible, read/write-protected storage area, and;

PRIOR TO ANY TRANSMISSION OF A CERTIFICATION REQUEST MESSAGE:

- generating by the on-board system a certification request (RCA) containing, in particular, a field of the public key (CA1, Kp) and usage indicators (U) of said public key,

- using said calculation means and said diversified key (KsMi) associated with this on-board system to calculate a cryptographic control value (Sc_i) on the entire request (RCA), said cryptographic control value being a digital signature calculated by means of the diversified private key (KsM_i);

WHEN A CERTIFICATION REQUEST IS SENT TO THE CERTIFICATION AUTHORITY BY THE ON-BOARD SYSTEM:

- forming a certification request message (MRCA) containing the request (RCA), the identifier (IDd_i) of the on-board system, the request message being constituted by the identification code (OP_j) of this authorized operator and by the serial number (SN_i) of the on-board system, and a cryptographic control value (Sc_i);

- transmitting to the certification authority (CA) said request message (MRCA) formed during the preceding phase and containing the public key (Kp) and the usage indicators (U) subject to said certification, and said cryptographic control value (Sc_i); and

WHEN A CERTIFICATION REQUEST MESSAGE (MRCA) IS RECEIVED BY THE CERTIFICATION AUTHORITY:

- retrieving the identification code of the authorized operator (OP_j) from the

digital data (IDd_i) of the on-board system,

- retrieving, from said identification code (OP_j) of said authorized operator, the value of the mother public key (KpM) as well as the identifier of the algorithm (CA1M) associated with the set (Lk) of the on-board system,

- verifying, from said mother public key (KpM), from said serial number (SN_i) of the on-board system, and from said certification request message (MRCA) received, said cryptographic control value (Sci), and establishing the authenticity of said cryptographic control value and the source of this certification request.

8. A method according to claim 7, characterized in that when the certification request (RCA) is generated by the on-board system, the method further comprises generating, at the on-board system level, a certification request (RCA), composed of three fields, including a public key algorithm identifier (CA1), a public key value (Kp), and an indicator of the usages of said key (U).

9. A method according to claim 7, characterized in that when the certification request is completed by the on-board system, the method further comprises the step of communicating a certification request template (GRCA) to said on-board system;

- checking, at the on-board system level, the syntax of the certification request template (GRCA) to ensure that it is a correctly formed certification request, and

- conditioning a step consisting of having the on-board system fill in missing fields of the certification request template (GRCA) to a positive verification.

10. A method according to claim 7, characterized in that, for a set of asymmetric signature keys (Kp), (Ks) generated by said on-board system, allowing use of the private key (Ks) under control of the cryptographic calculation means only for signature generation purposes, said private key (Ks) stored in said externally accessible read/write-protected storage area being unknown to the user and limited to a utilization exclusively for digital signature purposes, the utilization of said key being limited to signature purposes and the utilization of the certificate containing the corresponding public key being limited to signature verification purposes.

11. A method according to claim 7, characterized in that for a set of asymmetric keys, a public asymmetric encryption key (Ep) and a private asymmetric decryption key (Ds) generated by said on-board system, the method consists of associating, with said encryption and decryption keys (Ep), (Ds) and with the asymmetric decryption process, a symmetric "weak" decryption process and key, the symmetric decryption key being encrypted, then decrypted, by means of the private asymmetric decryption key (Ds), said private key (Ds) stored in said externally accessible read/write protected storage area being unknown to the user, so as to authorize the utilization of said key only for weak decryption purposes, the utilization of the certificate containing the corresponding public key being limited to said weak encryption purposes.

12. An on-board system comprising a card having a microprocessor, a RAM, a nonvolatile memory including a programmable memory and an externally accessible protected storage area memory, a cryptographic calculation module and an input/output system connected by a link of the BUS type,

- a diversified private key KsM_i stored in said externally accessible protected memory, said diversified private key, being unique and distinct for said on-board system and calculated from a mother private key KsM and an identification number of said on-board system, and being further associated with a mother public key KpM;

- said cryptographic calculation module comprising:

- means for calculating a signature from said diversified private key KsM_i, making it possible to calculate the signature of a certification request to certify a public key Kp associated with a private encryption key Ks or signature key, respectively, said private key Ks generated by said signature calculation means being stored in said externally accessible protected memory, said signature of a certification request being a function of the identification number of said on-board system, said signature calculation means making it possible to transmit to a certification authority a certification request message containing said certification request and said signature, which allows said certification authority to verify the source of the certification request from said on-board system and the protection of said diversified private key and private signature key in said externally accessible protected memory using only public elements, such as said mother public key KpM.--